

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Lean Marketing Inc.
52109 Copperwood Drive North, South Lyon, Michigan

Case: 2:16-mc-50716
Judge: Michelson, Laurie J.
Filed: 05-16-2016
SEALED MATTER (BG)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Eastern District of Michigan (identify the person or describe property to be searched and give its location):
Lean Marketing Inc.
52109 Copperwood Drive North, South Lyon, Michigan

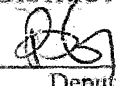
The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):
SEE ATTACHMENTS A and B

I hereby certify that the foregoing is
a true copy of the original on file in this
Office.

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

BY: 
Deputy

The search is related to a violation of 42 U.S.C. § 1320a-7b, and the application is based on these facts:
See the Affidavit.

☐ Continued on the attached sheet.

☒ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a. the basis of which is set forth on the attached sheet.

Applicant's signature

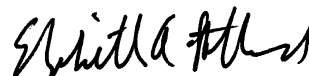
Paul M. Smith

Printed name and title

Sworn to before me and signed in my presence.

Date: 05/16/2016

City and state: Detroit, Michigan



ELIZABETH A. STAFFORD

Judge's signature

Elizabeth Stafford, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT

Under Seal

I, Paul M. Smith IV, being duly sworn and under oath, hereby state as follows:

1. I am a Special Agent with the United States Postal Service, Office of Inspector General and have been so employed since December 2012.
2. I currently specialize in the investigation of healthcare fraud. Prior to that, I was a Special Agent with the United States Department of Health and Human Services, Office of Inspector General for approximately eleven years. During my career, I have participated in investigations involving violations of federal law, including healthcare fraud, wire fraud, mail fraud, social security fraud, kickbacks and money laundering. Many of these investigations involved confidential informants, cooperating witnesses, and financial analysis. I have planned, organized, and participated in numerous search and arrest warrants.
3. The statements in this affidavit are based on my personal knowledge and experience, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purposes set forth above, I have not included each and every fact known to me concerning this investigation.

I. BASIS AND PURPOSE OF AFFIDAVIT

4. **Subject premises:** The purpose of this affidavit is to set forth probable cause for the issuance of a warrant for the search of the business location of Lean Marketing Inc., which is located at 52109 Copperwood Drive North, South Lyon, Michigan. Lean Marketing's registered

agent is Winnas Al-Sahli, and the subject premises are also her home address, which she shares with her husband, Eyad Khadr. The subject premises are further described in Attachment A.

5. **Statutes:** As set forth herein, probable cause exists to believe that there is evidence of violations of 42 U.S.C. § 1320a-7b (Anti-Kickback Statute) at the subject premises. The Anti-Kickback Statute, 42 U.S.C. § 1320a-7b(b), prohibits the solicitation or receipt of kickbacks in exchange for referring an individual to a person for items or services that may be paid for by a federal health care program. For example,

“[W]hoever knowingly and willfully solicits or receives any remuneration (including any kickback, bribe, or rebate) directly or indirectly, overtly or covertly, in cash or in kind to induce such person –

in return for referring an individual to a person for the furnishing or arranging for the furnishing of any item or service for which payment may be made in whole or in part under a Federal health care program . . .

shall be guilty of a felony. . . .”

There are certain payments that are specifically exempted from the reach of the Anti-Kickback Statute, including payments made to a bona fide employee for employment in the provision of covered services. 42 U.S.C. § 1320a-7b(b)(3). Other exemptions include returns on investment under specific circumstances, payments made pursuant to certain specified written services contracts, and payments made by a lessee to a lessor for the use of premises pursuant to certain specified written conditions. 42 C.F.R. § 1001.952.

6. **Summary:** Lean Marketing is an entity that pays recruiters or sales representatives for a group of compounding pharmacies in Indiana, Michigan, Wisconsin, and Illinois, among other locations. These pharmacies are all related in ownership, whether through individuals or LLCs owned by individuals. The pharmacies distribute a 5- to 7-ingredient

compounded cream for which the pharmacies bill federal healthcare programs. One month's supply of the cream for one patient costs the federal healthcare programs anywhere from approximately \$1,800 to \$18,000, depending upon the program and how the pharmacy submits its bills for the cream. The variation in price depends in large part on the cream's ingredients. Nowscript LLC is one of those pharmacies. Lean Marketing is located at the home of Nowscript's manager, Eyad Khadr, and Lean Marketing's registered agent is his wife, Winnas Al-Sahli. The investigation to date has revealed that the pharmacies use Lean Marketing to pay kickbacks to recruiters or sales representatives, some of whom, in turn, pay kickbacks to prescribers, all to refer patients to the pharmacies, who bill the federal healthcare programs described below – in violation of the Anti-Kickback Statute, 42 U.S.C. § 1320a-7b.

II. FEDERAL HEALTH CARE PROGRAMS AND BILLING FOR COMPOUNDED DRUGS

7. **Medicaid:** Medicaid is a federally assisted grant program for the states. Medicaid enables states to provide medical assistance and related services to needy individuals. The Centers for Medicare and Medicaid Services (CMS), which is a component of the U.S. Department of Health and Human Services, administers Medicaid on a federal level. Within broad federal rules, however, each state decides who is eligible for Medicaid, the services covered, payment levels for services, and administrative and operational procedures. The state directly pays the providers of Medicaid services, with the state obtaining the federal share of the payment from the accounts drawn on funds of the United States Treasury. The federal share in Indiana is approximately two-thirds; the state share is one-third. The State of Indiana, through its Family and Social Services Administration, Office of Medical Policy and Planning, participates in the Medicaid Program. Indiana Medicaid is a federal health care benefit program.

8. **Medicare:** Medicare is a federally funded program that provides medical services, equipment, and supplies to the elderly, blind, and disabled, pursuant to the Social Security Act. CMS, in addition to administering Medicaid together with states, also administers Medicare. Medicare has several parts, which include hospital insurance (Part A), medical insurance (Part B), and prescription drug insurance (Part D).

9. Enrolled providers of medical services to Medicare and Medicaid patients are eligible for reimbursement for covered services under the provisions of the Social Security Act. By becoming a participating provider in Medicaid and Medicare, enrolled providers agree to abide by rules, regulations, policies, and procedures governing reimbursement, and to keep and allow access to records and information as required by Medicare and Medicaid. In order to receive funds, enrolled providers, together with authorized agents, employees, and contractors, are required to abide by all provisions of the Social Security Act, the regulations promulgated under the Act, and applicable policies and procedures issued by the State of Indiana.

10. **Department of Labor Office of Workers' Compensation Programs:** The Federal Employee Compensation Act (FECA) is a federally funded health care program as described in 20 C.F.R. § 10.0, that provides monetary compensation, medical care, and vocational rehabilitation to civilian employees of the United States Government, including Postal Service employees, for disability due to personal injury or disease sustained while in the performance of duty. The FECA program is administered by the Department of Labor, Office of Workers' Compensation Programs (DOL-OWCP) located in 12 district offices throughout the United States. It is financed by the Employees' Compensation Fund, which consists of funds appropriated by Congress directly, or indirectly through a charge back system and administrative

fees to various federal agencies, including the U.S. Postal Service. FECA is a federal health care program.

11. **Compounding:** According to the Food and Drug Administration (FDA), pharmacy compounding involves the preparation of medication by combining and mixing different types and dosages of ingredients to create a drug or medication tailored to the needs of an individual patient and for which there is no equivalent form commercially available. Pharmacies preparing and dispensing compound drugs and medications are required to create and maintain compound logs identifying the various ingredients used to create the compound drug or medication.

12. **NDC numbers and billing:** The Drug Listing Act of 1972 requires registered drug establishments to provide the FDA with a current list of all drugs manufactured, prepared, propagated, compounded, or processed by it for commercial distribution. 21 U.S.C. § 360. Drug products are identified and reported using a unique, three-segment number, called the National Drug Code (NDC), which serves as a universal product identifier for drugs. In particular, the NDC number is a ten-digit number that serves to identify various aspects of a drug, including the particular version of the drug, as well as its manufacturer. NDC numbers are used for the billing of drugs or medications.

13. Typically, Medicare and Indiana Medicaid reimburse pharmacies for compounded creams dispensed based on the NDC number of the drugs or medications contained in the compounded cream. For compound drugs and medications, the NDC numbers submitted on a claim are required to match the numbers submitted on a claim for the ingredients that were in fact used to create the compound drug or medication that is dispensed. DOL-OWCP pays for compounded medications that are medically necessary and ordered by a medical professional.

Compounded medications are reimbursed if the NDC numbers are appropriate and consistent with the standard of care for the patient's injuries.

III. THE PHARMACIES ASSOCIATED WITH LEAN MARKETING

14. This case involves at least 4 compounding pharmacies in Michigan and Indiana, which are hereinafter referred to as "the pharmacies." They are related through ownership, but the individual owners typically hold their ownership interests through LLCs that they have formed, as described below.

15. According to public records and bank records, Lean Marketing is located at the subject premises. As explained below, Lean Marketing is an entity that pays recruiters or sales representatives who work for the pharmacies. Winnas Al-Sahli is the registered agent, and her husband, Eyad Khadr, is the manager of Script LLC, DBA Nowscrip, a compounding pharmacy located in Sterling Heights, Michigan.

16. According to a former employee of Nowscrip, Eyad Khadr had no pharmacy background, license, or formal training. The former employee stated that Eyad Khadr focused the pharmacy's business on workers' compensation because the pharmacy would get paid more by that health care program for the compounded cream. Eyad Khadr mentioned having contracts with doctors relating to the prescribing of the compounded creams. Finally, the former employee stated that sometimes insurance companies and health care programs denied a formulation that was submitted for pre-approval. Rather than contacting the prescriber and having the prescriber approve a new formulation, the pharmacy would simply omit the ingredients that were not covered by insurance, and resubmit the claim. Khadr typically used his cell phone to conduct pharmacy business.

17. According to tax records, Nowscript is owned by two LLCs: MD Medical Distribution LLC and PNK Services LLC. In turn, those two LLCs are owned as follows:

- MD Medical Distribution LLC: Owned by Manny Bojorquez, a California resident, and Duke Zukowski, a North Carolina resident;
- PNK Services LLC: Owned by Sarah Patel, Christy Patel, Neil Patel, and Ziad Khader. According to bank records, it is located at Ziad Khader's home in Carmel, Indiana.

18. Ziad Khader is Eyad Khadr's brother. Ziad, through PNK Services LLC, as well as several other LLCs, owns not only Nowscript, but the following additional compounding pharmacies: Valuscript (the DBA for Khader David Pharmacy Services LLC, located in Carmel, Indiana – now closed); Myscript LLC (located in Taylor, Michigan – now closed); and Proscript LLC (located in Indianapolis, Indiana). Federal agents executed search warrants at Ziad Khader's residence, as well as at Proscript, on March 31, 2016. Evidence from these searches includes text message conversation between Ziad Khader and Eyad Khadr about Valuscript and Nowscript, among other things.

19. Eyad Khadr is also the registered agent for CustomScript LLC, a compounding pharmacy. According to state records, CustomScript LLC lists the subject premises as a place of business.

20. According to an April 21, 2016 interview with Delfin David, a part-owner of Valuscript, Lean Marketing is the entity that pays individuals who generate prescriptions for the compounded cream on behalf of Valuscript. David did not provide an explanation beyond this as to how they were paid, or how these individuals generated the prescriptions.

IV. EVIDENCE OF KICKBACKS PAID FROM THE PHARMACIES THROUGH OR FACILITATED BY LEAN MARKETING

21. Lean Marketing is connected to sales reps who worked for Valuscript and Ziad Khader. Evidence obtained from the search of Ziad Khader's house includes text messages between Ziad Khader and individuals who acted as sales representatives. One example is a text message conversation between Ziad and Jeff Buttitta. On October 16, 2015, agents interviewed Buttitta, a Fishers, Indiana resident and former golf pro. He worked as a sales representative for Valuscript, and he incorporated JMB Medical, LLC, which was the entity through which he received compensation from Valuscript. Buttitta was paid a percentage of the money received by Valuscript from insurance and federal health care programs, for prescriptions written by doctors whom he had visited.

22. According to Buttitta, each doctor he was able to induce to write prescriptions for the compounded cream was "tagged" as one of his doctors through Lean Marketing, which was controlled by Ziad Khader and the other owners of the pharmacies. The pharmacies kept track of each sales representative and each representative's doctors. Representatives like Buttitta were able to log in and check their commissions. According to the pharmacy's bank records, Buttitta was paid approximately \$49,118 by Myscript from June 2013 through March 2016. He believed that Valuscript and Myscript, as well as Proscript, were all related. He reported to Ziad Khader. Buttitta believed that the owners routed the compounded cream prescriptions to different pharmacies depending on which federal healthcare program or private insurance company was being charged.

23. The text messages between Ziad Khader and Buttitta include the following:

3883 Instant
Messages

11/13/2014 From: +13177102500
11:59:44 AM(UTC-5) Jeff Buttitta

Ziad, I did not hear back from you but wanted to be sure I will still be getting credit for my docs writing scripts. Lean marketing has been updating my commission. As I said before, I still hope to do business with you direct.
Source Extraction: Logical

4639 Instant
Messages12/1/2014
8:53:07 AM(UTC-
5)From: +13177102500
Jeff ButtaHi Ziad. Checking in to see if tomorrow still
works to meet? Also my lean report went
down shows 44 scripts paying me a
commission of \$788.50 for November. Thx.
Source Extraction: Logical

24. Lean Marketing and Eyad Khadr are also directly connected to a business called MD Medical Distribution. As mentioned above, according to tax records, Nowscrip, the pharmacy Eyad Khadr manages, is part-owned by MD Medical Distribution LLC, DBA DynaMD, a California corporation. MD Medical Distribution LLC, in turn, is part-owned by Manny Bojorquez, a California resident. According to bank records, Lean Marketing paid MD Medical Distribution approximately \$739,420 from March 2014 through May 2014. MD Medical Distribution was also paid by Myscript, Nowscrip, and Valuscript.

25. On October 15, 2015, agents interviewed Catrina Gorny, an Illinois resident. She works as an independent contractor for DynaMD, the DBA name for MD Medical Distribution. According to Gorny, she has only been to the MD Medical Distribution office in California once, when she was first hired. Her role with MD Medical Distribution involves functioning as a go-between connecting doctors to Nowscrip, a compounding pharmacy in Michigan, as well as another pharmacy. Gorny described herself as a customer service representative who maintains Nowscrip's relationship with doctors. Gorny stated that she rarely communicates with Nowscrip, except on occasions when the pharmacy contacts her to ask a doctor for a letter of medical necessary, or to ask a doctor for missing documentation relating to the prescriptions. In those instances, Gorny contacts the doctor, if it is a doctor she connects to Nowscrip, and makes that request.

25. Gorny stated that, in her role with MD Medical Distribution, she delivers a monthly commission check to the doctors described above, *i.e.*, the doctors she connects to Nowscrip. Gorny stated that the doctors receive those commissions for the compounded creams

they prescribe. Gorny was not aware of the specific percentage of the commission, but she knew the commissions were based on what insurance paid Nowscript.

26. Gorny stated that she receives a salary of approximately \$1,500 every two weeks, as well as additional commission payments of approximately 1% of the net profit from the amount of compounded cream prescribed by the doctors she calls upon. Gorney's supervisor is Manny Bojorquez.

27. On October 14, 2015, agents interviewed Manny Bojorquez. Bojorquez had initiated contact telephonically with the agents after Catrina Gorny notified him that agents had left her a voicemail message. Bojorquez acknowledged that he owned MD Medical Distribution. He said that MD Medical Distribution was paid 45% of the net profit Nowscript Pharmacy made from the compounded creams prescribed by physicians he recruited. He estimated that that percentage equaled approximately \$30,000 to \$60,000 per month. Bojorquez paid his customer sales representatives, including Gorny, a percentage of the revenue from those compounded cream sales. While he denied paying any doctor to prescribe the compounded cream, bank records for MD Medical Distribution reveal payments of approximately \$1.4 million to Medical Access Group, a medical therapy practice that employs doctors; approximately \$800,000 to a Dr. Robert Fink; approximately \$858,000 to a Dr. Ron Silver, and several other payments to medical groups, all from July 2012 through December 2015.

28. Bojorquez is connected to Lean Marketing through more than just payments from Lean Marketing to his business. Text messages between Ziad Khader and Neil Patel, a co-owner of Nowscript and other related compounding pharmacies, indicate the following:

3/25/2014 12:49:59 PM(UTC-4), +13175074544 (Neil Patel)

Are we paying manny's Valuscript scripts out of lean or should take the money out of Valuscript and pay him out of myscript?

Status: Read

Read: 3/25/2014 2:01:14 PM(UTC-4)

29. The three related pharmacies (Nowscript, Myscript, and Valuscript) billed DOL-OWCP, a federal healthcare program, for the prescriptions written from the prescribers mentioned in the paragraphs above as connected to MD Medical Distribution. The billings resulted in at least \$11.6 million being paid to the three pharmacies from DOL-OWCP, from approximately October 2013 through March 2015. Valuscript and Nowscript also billed Medicare for the compounded creams, while Valuscript and Proscript billed Indiana Medicaid for the same.

V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

30. As described above and in Attachment B, this application seeks permission to search for records that might be found on the subject premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

31. *Probable cause.* I submit that if a computer or storage medium is found on the subject premises, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In

addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."
- e. Based on actual inspection of other evidence related to this investigation, I am aware that computer equipment was used to generate, store, and print documents used in the scheme. There is reason to believe that there is a computer system currently located on the subject premises.

32. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the subject premises because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user’s state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner’s motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a “wiping” program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).
- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can

be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

33. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

- a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.
- b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises.

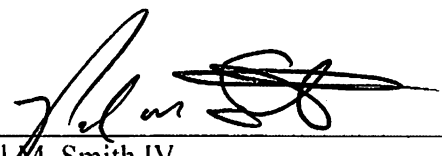
However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

- c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VI. REQUEST FOR ISSUANCE AND SEALING OF SEARCH WARRANT

35. There is probable cause to believe that evidence of violations of 42 U.S.C. § 1320a-7b exists at the subject premises, which is more particularly described in Attachment A. I request that a Search Warrant be issued directing any Special Agent of the U.S. Postal Service, Office of Inspector General, along with any other Federal, state, or local law enforcement officers or investigators, to enter and search the subject premises, as well as to seize the items set forth in Attachment B. Because this is an ongoing investigation, I request that the search warrant be sealed.



Paul M. Smith IV
Special Agent
U.S. Postal Service, Office of Inspector General

Subscribed and sworn to before me this 11th day of May, 2016.


ELIZABETH A. STAFFORD

ELIZABETH A. STAFFORD
United States Magistrate Judge
Eastern District of Michigan

Attachment A

The premises are located at 52109 Copperwood DR N, South Lyon, MI, 48178, further described as a two story dark red brick with beige vinyl siding. Residence is located on the south side of Copperwood DR N, near the intersection of Copperwood DR N and Tamarack DR. The front entrance is facing north with an enclosed archway porch and beige front door. The garage entrance is facing east. A gazebo is visible on west side of residence; an open field with no residence or structure is located adjacent to the west side of the residence. The address number 52109 is embedded in the brick of the garage.



ATTACHMENT B

Property to be seized

All records relating to violations of 18 U.S.C. § 1347 and 42 U.S.C. § 1320a-7b, or involving Proscript, Valuscript, Nowscrip, Myscript, Lean Marketing, and any related individuals or entities (such as owners of the foregoing entities, other pharmacies, sales representatives, or sales representatives' companies), occurring after August 1, 2011, including:

1. Management and organizational charts, personnel data, and/or other documents sufficient to identify and describe the operation of the entities mentioned above, including:
 - a. Corporate structure, including relationships to parents, subsidiaries, divisions, joint ventures, or and any related entities.
 - b. The management structure and all personnel.
 - c. All employment or payroll records to include records disclosing the dates of employment, wages or commissions paid, checks (front and back). Employees Withholding Exemption Certificates (Forms W-4); Wage and Tax Statement (Forms W-2) disclosing annual wages; U.S. Information Returns (Forms 1099); Schedules K-1; disclosing fees, commissions, etc. paid; licenses, accreditations, or training completed by employees or contractors.
2. All current and former suppliers, wholesalers, or distributors, and their corresponding contact information, including points of contact, addresses, phone numbers, and email addresses.
3. All inventory records, including those establishing beginning and ending inventories including inventory sheets, work-papers, logged formula worksheets, Universal Claim Form for Compounded Medication, compounding worksheets, signature logs for prescriptions or delivery manifests, and valuation records; records and work-papers reflecting the purchase of drugs, associated pedigree, wholesaler/distributor contracts, and NDC pricing.
4. All purchase detail or wholesaler confirmation reports, to include invoice number, purchase date, NDC, medication, package size, and quantity purchased/returned of pharmaceutical products purchased.
5. Records and information relating to billing and enrollment in healthcare programs, including claims, manuals, instructions, and policies.

6. Any correspondence – internal and external – relating to audits or inspections.
7. Records and information relating to instructions, guidance, advice, and training for health care statutes, regulations, and compliance.
8. Records and information, including correspondence, relating to recruiters, marketers, consultants, sales representatives, or any other individual or entity associated with the referral of accounts or patients for health care services.
9. All correspondence relating to compounded creams submitted for reimbursement to federal health care programs.
10. Records and information relating to the finances of the individuals and entities mentioned above.
11. Monetary instruments or cash exceeding \$500.
12. Any safe, strongbox, lockbox, and/or other container used, designed, or intended to secrete or secure valuables and/or property from disclosure or taking, including keys, and any and all documents and records relating thereto.
13. Computers or storage media used as a means to commit the violations described above. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

AUSA: Michael C. Martin, (313) 226-9670

AO 93 (Rev. 11/13) Search and Seizure Warrant


Special Agent: Paul M. Smith

UNITED STATES DISTRICT COURT

for the
Eastern District of MichiganIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)Lean Marketing Inc.
52109 Copperwood Drive North, South Lyon, MichiganCase:2:16-mc-50716
Judge: Michelson, Laurie J.
Filed: 05-16-2016
SEALED MATTER (BG)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of
the following person or property located in the Eastern District of Michigan
(Identify the person or describe the property to be searched and give its location):Lean Marketing Inc.
52109 Copperwood Drive North, South Lyon, MichiganI hereby certify that the foregoing is
a true copy of the original on file in this
Office.
CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF MICHIGANBY: 
DeputyI find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or
property described above, and that such search will reveal (Identify the person or describe the property to be seized)

See Attachments A and B

YOU ARE COMMANDED to execute this warrant on or before May 30, 2016 (not to exceed 14 days)
in the daytime 6:00 a.m. to 10:00 p.m. at any time in the day or night because good cause has been
established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to
the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as
required by law and promptly return this warrant and inventory to**Duty Magistrate Judge**
(United States Magistrate Judge)Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)✓ for 30 days (not to exceed 30) until, the facts justifying, the later specific date of _____

Date and time issued:

MAY 16 2016

02:35pm

ELIZABETH A. STAFFORD
Judge's signature

City and state:

Detroit, Michigan

Elizabeth A. Stafford, United States Magistrate Judge

Printed name and title

Return

Attachment A

The premises are located at 52109 Copperwood DR N, South Lyon, MI, 48178, further described as a two story dark red brick with beige vinyl siding. Residence is located on the south side of Copperwood DR N, near the intersection of Copperwood DR N and Tamarack DR. The front entrance is facing north with an enclosed archway porch and beige front door. The garage entrance is facing east. A gazebo is visible on west side of residence; an open field with no residence or structure is located adjacent to the west side of the residence. The address number 52109 is embedded in the brick of the garage.



ATTACHMENT B
Property to be seized

All records relating to violations of 18 U.S.C. § 1347 and 42 U.S.C. § 1320a-7b, or involving Proscript, Valuscript, Nowscript, Myscript, Lean Marketing, and any related individuals or entities (such as owners of the foregoing entities, other pharmacies, sales representatives, or sales representatives' companies), occurring after August 1, 2011, including:

1. Management and organizational charts, personnel data, and/or other documents sufficient to identify and describe the operation of the entities mentioned above, including:
 - a. Corporate structure, including relationships to parents, subsidiaries, divisions, joint ventures, or and any related entities.
 - b. The management structure and all personnel.
 - c. All employment or payroll records to include records disclosing the dates of employment, wages or commissions paid, checks (front and back). Employees Withholding Exemption Certificates (Forms W-4); Wage and Tax Statement (Forms W-2) disclosing annual wages; U.S. Information Returns (Forms 1099); Schedules K-1; disclosing fees, commissions, etc. paid; licenses, accreditations, or training completed by employees or contractors.
2. All current and former suppliers, wholesalers, or distributors, and their corresponding contact information, including points of contact, addresses, phone numbers, and email addresses.
3. All inventory records, including those establishing beginning and ending inventories including inventory sheets, work-papers, logged formula worksheets, Universal Claim Form for Compounded Medication, compounding worksheets, signature logs for prescriptions or delivery manifests, and valuation records; records and work-papers reflecting the purchase of drugs, associated pedigree, wholesaler/distributor contracts, and NDC pricing.
4. All purchase detail or wholesaler confirmation reports, to include invoice number, purchase date, NDC, medication, package size, and quantity purchased/returned of pharmaceutical products purchased.
5. Records and information relating to billing and enrollment in healthcare programs, including claims, manuals, instructions, and policies.

6. Any correspondence – internal and external – relating to audits or inspections.
7. Records and information relating to instructions, guidance, advice, and training for health care statutes, regulations, and compliance.
8. Records and information, including correspondence, relating to recruiters, marketers, consultants, sales representatives, or any other individual or entity associated with the referral of accounts or patients for health care services.
9. All correspondence relating to compounded creams submitted for reimbursement to federal health care programs.
10. Records and information relating to the finances of the individuals and entities mentioned above.
11. Monetary instruments or cash exceeding \$500.
12. Any safe, strongbox, lockbox, and/or other container used, designed, or intended to secrete or secure valuables and/or property from disclosure or taking, including keys, and any and all documents and records relating thereto.
13. Computers or storage media used as a means to commit the violations described above. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, “COMPUTER”):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;
 - d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
 - e. evidence indicating the computer user’s state of mind as it relates to the crime under investigation;

- f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. evidence of the times the COMPUTER was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. records of or information about Internet Protocol addresses used by the COMPUTER;
- l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- m. contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.